Glossary

A records — Host name to IP address mappings in the DNS database that are used in host name resolution.

Accounting provider — Server (typically a RADIUS server) that logs the activity and connection time for a remote user. This is often used to charge remote clients for online time, as in the case of an ISP providing Internet service.

active directory integrated zones — DNS zones stored in the Active Directory database and replicated along with other Active Directory information.

Active Directory (AD) services — Enterprise-level directory service designed to combine domain structures into a manageable, extensible, network structure.

Active Directory Users and Computers — Tool used to configure the objects in the Windows 2000 Active Directory. Among other things, you use this tool to configure the properties of user accounts. Dial-in properties for a user include whether the user may dial in to the RRAS server and whether a callback number should be used.

Address Resolution Protocol (ARP) — Low-level protocol that resides within the IP protocol. It is used as a way of resolving IP addresses to MAC addresses.

Advanced Research Projects Agency Network (ARPANet) — Original name for the Internet; ARPA was the government agency responsible for sponsoring the research that lead to the TCP/IP protocol stack and the modern-day Internet.

ANDing — Logically combining binary numbers; the results are similar to multiplying binary numbers; ANDing a 1 and a 1 gives a 1. All other combinations (1 and 0, and 0 and 0) result in 0.

Application Programming Interface (API) — Standardized set of commands and programming parameters used to simplify the interaction between applications and lower-level networking components.

areas — OSPF division of the internetwork into collections of contiguous networks that help keep routing tables from growing too large. Each router only keeps a link-state database for those areas connected to the router.

area border routers — OSPF router that has an interface in more than one OSPF area.

Asynchronous Transfer Mode (ATM) — Cell-based LAN/WAN networking technology that can handle voice, video, and data traffic; Windows 2000 provides native ATM support.

attributes — Specific values associated with an object; an example is the attribute of First or Last name for the User object.

authentication — Process of verifying a user's credentials so that the user may log on to the system. Authentication is normally performed using a username and password. Authentication may be unencrypted (clear text) or use any of a number of **encryption** types.

authority — Ability to control what resource records, subdomains, and other attributes are associated with a particular DNS domain.

Automatic Private IP Addressing (APIPA) — New feature in Windows 98 and Windows 2000 that allows DHCP clients to select an IP address from the private range 169.254.0.0/16 whenever they cannot find a DHCP server on the local segment.

autonomous system — One in which a set of networks and routers are all under the same administration.

b-node — NetBIOS node type that uses broadcasts to resolve NetBIOS names to IP addresses.

backbone area — OSPF areas connected by a special type of area called a backbone area.

backbone router — Any router configured in an OSPF backbone area.

Bandwidth Allocation Control Protocol (BACP) — *See* Bandwidth Allocation Protocol (BAP).

Bandwidth Allocation Protocol (BAP) — Together with the Bandwidth Allocation Control Protocol (BACP), allows a client to add and remove links dynamically during a multilink session to adjust for changes in bandwidth needs.

binary format — IP address displayed as four sets of eight binary numbers separated by periods.

binding — Associating or connecting a network layer protocol (or even a network service) to a specific network interface card.

BootP — Older alternative to DHCP that diskless workstations used to obtain IP addresses.

Border Gateway Protocol (BGP) — Newer and more powerful exterior routing protocol that has largely replaced the older Exterior Gateway Protocol.

boundary layers — Layers in the Windows 2000 networking architecture that act as intermediaries between upper layers, the network protocols, and lower layers of the model.

broadcast domain — That portion of a network where broadcasts are propagated; normally broadcast domains are created by router placement in a network.

caching-only servers — DNS server configured without any zone files; a caching-only server contains IP addresses of DNS servers it can query to answer client requests and then store the information in a local cache.

certificates — Allows verification of the claim that a given public key actually belongs to a given individual. This helps prevent an impersonator from using a phony key.

Certificate Authority (CA) — Any trusted source willing to verify the identities of people to whom it issues certificates and to associate those people with certain public and private keys.

certificate enrollment — Process whereby a client obtains a certificate from a certificate authority.

Certificate Revocation Lists (CRL) — List of revoked certificates and the codes defining the reasons for revocation.

certificate services — Networking service in Windows 2000 that creates and manages a public key infrastructure within an organization.

Certificate Store — Database created during the installation of a CA. Installed certificate services on an Enterprise root CA, creates the store in the Active Directory. If installing services on a Standalone root CA creates the store on the local server.

Certificate Trust List (CTL) — Holds the set of all root CAs whose certificates users and computers can trust.

Challenge Handshake Authentication Protocol (CHAP) — Type of authentication in which the authentication agent sends the client program a key for encrypting the username and password.

clustering support — Ability of an operating system to connect multiple servers in a fault-tolerant group. If one server in the cluster fails, all processing continues on another server. Clusters ensure high availability and reliable performance.

converged — Status of an internetwork when all its routers have the correct routing information in their tables.

Convergence time — When a link or router fails, the time taken for all routers on the network to reconfigure themselves with the proper information.

Data Link Control (DLC) — Nonroutable protocol used mainly to connect to Hewlett-Packard printers using Jet Direct network cards.

dead gateway detection — Feature of Windows 2000 that allows a machine to detect

when a default gateway is unreachable and then switch to a configured back-up default gateway.

decrypt — Process of decoding encrypted data.

default gateway — IP address of the router port to networks outside the local network.

demand-dial interfaces — Interface configured in RRAS that can dial a remote router whenever a connection needs to be made.

demand-dial routing — Allows an RRAS server configured as a router to dial-up a remote router whenever it needs to send messages to that router.

DHCP Allocator — Simplified version of a DHCP server used by NAT to assign IP addressing information automatically to clients on the private network.

DHCP relay agent — Software component loaded via Routing and Remote Access Service to a Windows 2000 machine; allows a machine to act as a proxy for DHCP clients on a segment.

DHCPAcknowledgment — Packet broadcast by a DHCP server to a DHCP client that grants the client a lease for a particular IP address; fourth step of four-step DHCP lease process.

DHCPDiscover — Packet broadcast by DHCP clients to find DHCP servers on the local segment; first step of four-step DHCP lease process.

DHCPNack — Negative acknowledgment that a DHCP server broadcasts if it must decline a client's request for a particular IP address.

DHCPOffer — Packet broadcast by a DHCP server to a DHCP client that contains a possible IP address for lease; second step of four-step DHCP lease process.

DHCPRequest — Packet broadcast by a DHCP client requesting the IP address offered in a DHCPOffer packet; third step of four-step DHCP lease process.

Dial-Up Networking — Name given to the process and interface that most versions of Microsoft Windows use to dial in to a remote server.

DNS proxying — Method of relaying DNS name resolution requests from clients on a private network through the NAT server to a DNS server on the Internet.

DNS zone file — Text file, stored on a DNS server, that contains all information and resource records for a particular zone.

DNS zones — Portion of the DNS namespace that can be administered as a single unit.

Domain Name System (DNS) — Hierarchical naming system used to resolve host name to IP address mapping. It contains resource records.

dotted decimal — IP addresses displayed as a series of four decimal numbers separated by periods, for example, 192.168.12.2.

dynamic assignment — Configuring a host to obtain an IP address automatically using DHCP.

Dynamic Domain Name System (DDNS) — Extension to the DNS systems that allows dynamic updates to the DNS database. The Windows 2000 DHCP server service can integrate with DDNS to allow dynamic DNS registration for clients that receive dynamic IP addresses.

Dynamic Host Configuration Protocol (DHCP) — Protocol used to automatically assign IP addressing and other TCP/IP information to clients. DHCP is considered easier and more reliable than manual addressing.

dynamic mappings — Created when users on the private network initiate traffic with a public Internet location. The NAT service automatically translates the IP address and source ports and adds these mappings to its mapping table.

dynamic router — Routers that automatically share their routing information with other routers on the network using a router protocol such as RIP or OSPF.

EFS Recovery Key — Spare private encryption key capable of decrypting the data. The key maps to a trusted account called a Recovery Agent.

Encrypting File System (EFS) — Protocol Windows 2000 to uses encrypt data on a computer by combining the data in those files with the public key certificate of the user logged on to the computer.

Encryption — Process of translating information into an unreadable code that can only be translated back (decrypted) by using a secret key or password.

enhanced security — Increased security measures available in Windows 2000 via the inclusion of Kerberos version 5 security and IP security.

Ethernet — Most widely used networking architecture; contention-based architecture that uses carrier sense multiple access/collision detection as its access method.

Enterprise CA — Acts as a CA for an enterprise and requires access to the Active Directory.

event logging — Most applications in Windows (and Windows itself) log events to a file. Events are bits of information and any errors generated by these applications. Once logged, you can view the events using the Event Viewer utility.

Extensible Authentication Protocol (EAP) — General protocol for PPP authentication that supports multiple authentication mechanisms. Instead of selecting a single authentication method for a connection, EAP can negotiate an authentication method at connect time.

Exterior Gateway Protocol (EGP) — Exterior routing protocol used to connect different autonomous systems.

Fat allocation table (FAT) 32 support — Ability of an operating system to read, write, and otherwise fully support the new version of the file allocation table file system introduced in the Win9x product family.

File Transfer Protocol (FTP) — Provides for file transfer between two TCP/IP hosts; uses TCP as its transport protocol.

filter action — Actions assigned to a connection whose properties match an associated list of filters. Typical actions are to accept and block connections or to negotiate security for the connection.

filter list — List of filters assigned to a rule. Connections whose properties match the list of filters have an associated filter action applied to them.

forward lookup zones — DNS zone files that hold resource records that map host names to IP addresses. (They can also hold various other resource records.)

Fully Qualified Domain Name (FQDN) — Entire name of a host that includes the host name and the domain name; for example, host1.win2k.org signifies the computer host1 in the win2k.org DNS domain.

global options — Options that apply to all clients in all scopes configured on a DHCP server.

group NetBIOS names — NetBIOS names used to register entire groups of computers; an example is domain controllers in a domain.

h-node — NetBIOS node type that first attempts directed communication to a WINS server to resolve NetBIOS names to IP addresses; if directed communication fails, clients with this node type then try a broadcast to resolve NetBIOS names to IP addresses.

hop — Each router that a packet of information must pass between its source and destination hosts. The number of hops is also referred to as metric count or metric cost.

host ID — Portion of an IP address that represents the bits used for host identification.

host files — Text files that contain host name to IP address mapping; used to perform host name to IP address resolution. Precursor to the DNS system.

host names — Common names given to network devices to allow users to interact with a name instead of an IP address.

hostname — Command used after the command prompt to display the host name of the local machine.

in-addr.arpa — Name given to the reverse lookup zone file.

indirect routing — Occurs when a packet of information must pass over a router at some point between its source and destination.

Internet Assigned Numbers Authority (IANA) — Group responsible for controlling allocation of IP addresses to the Internet community.

Internet Connection Sharing (ICS) — Simplified version of the NAT protocol that is easy to configure and manage and is available in Windows 98, Windows Millennium Edition, Windows 2000 Server, and Windows 2000 Professional. ICS is not as configurable as NAT.

Internet Control Message Protocol (ICMP) — Handles the communication of errors and status messages within the TCP/IP protocol stack.

Internet Group Management Protocol (IGMP) — Standard protocol for IP multicasting over the Internet. It is used to establish host memberships in particular multicast groups.

Internet Protocol (IP) — Connectionless, best-effort delivery protocol in the TCP/IP protocol stack that handles routing of data and logical addressing with IP addresses.

Internet Protocol version 6 (IPv6) — Advanced version of the Internet Protocol that uses 128-bit addresses in hexadecimal format.

Internet Service Providers (ISPs) — Companies that provide access to the Internet backbone.

Internetwork Packet eXchange (IPX) — Connectionless, layer three protocol that provides routing function for the IPX/SPX protocol stack.

Internetwork Packet eXchange/Sequenced Packet eXchange (IPX/SPX) — Routable protocol stack designed by Novell to provide networking services for the Netware network operating system.

inverse query — DNS query attempting to resolve a host name from a known IP address.

IP (Internet Protocol) — Network layer protocol of the TCP/IP protocol suite that is responsible for routing packets between hosts.

IP address — 32-bit logical addresses that must be assigned to every host on a TCP/IP network.

IP Security (IPSec) — Set of protocols that supports the secure exchange of data at the IP layer. In RRAS, IPSec is used in conjunction with L2TP in the formation of Virtual Private Networks.

ipconfig — Command-line tool used to verify IP settings; can also be used to renew or release dynamically assigned IP addresses and DNS information.

IPSec client — Computer that initiates the IPSec connection.

IPSec driver — IPSec component that actually encrypts and decrypts data using keys prepared by the ISAKMP/Oakley Service, and sends the data between computers.

IPSec policies — Sets of rules assigned to clients that define how those clients use IPSec.

IPSec policy agent service — IPSec component responsible for retrieving the computer's assigned IPSec policy from the Active Directory.

IPSec server — Computer that responds to an IPSec connection.

IPX (Internetwork Packet eXchange) — Networking protocol developed by Novell for use primarily with their NetWare operating systems. Since NetWare is such a popular network operating system, most other operating systems, such as Microsoft Windows, provide an IPX-compatible networking protocol. In Windows 2000, this IPX-compatible protocol is named NWLink.

ISAKMP/Oakley Service — IPSec component that creates the security association between communicating computers and is also responsible for generating the keys used to encrypt and decrypt the data sent over the IPSec connection.

iterative query — DNS query to which the server responds with the best answer it can provide or by forwarding the request to another name server and then returning an answer.

Kerberos version 5 — Shared secret key encryption mechanism used to provide security for authentication sessions in a Windows 2000 network.

Layer-Two Tunneling Protocol (L2TP) — Extension of the PPP remote access protocol; one type of tunneling protocol used to form Virtual Private Networks.

Link control protocol (LCP) — LCP extensions include a number of enhancements to the LCP protocol used to establish a PPP link and control its settings. One of the primary enhancements included is the ability for the client and server to agree dynamically on protocols used on the connection.

LMHOSTS — Text file mapping NetBIOS names to IP addresses; precursor to WINS service.

local area network (LAN) — Network confined within a small area such as a single building or a small campus.

m-node — NetBIOS node type that first attempts broadcasts to resolve NetBIOS names to IP addresses; if broadcasts fail, the client then tries directed communication with the WINS server.

Media Access Control (MAC) address — Physical address burned in the EPROM on a network card when it is manufactured.

member scopes — Scopes joined together in superscopes.

Microsoft Certificate Server (MCS) — Windows 2000 component that acts as an authority for issuing and managing certificates.

Microsoft CHAP (MS-CHAP) — Modified version of CHAP that allows the use of Windows 2000 authentication information. There are two versions of MS-CHAP. Version 2 is the most secure, and all Microsoft operating systems support it. Other operating systems sometimes support version 1.

Microsoft Management Console (MMC) — Extensible framework within which Windows 2000 management snap-ins such as the DHCP snap-in reside.

mixed mode — Mode that Windows 2000 domain controllers use when the network consists of Windows 2000 servers and Windows NT servers (or machines not Active Directory-aware). All Windows 2000 servers run in mixed mode by default. You must manually change them to native mode.

multicast routing — Targeted form of broadcasting that sends messages to a select group of users instead of all users on a subnet.

multicast scopes — Ranges of multicast addresses configured to be dynamically assigned to host via DHCP.

multicasting — Broadcasting packets to only certain hosts on a TCP/IP network.

multi-homed — Any computer configured either with multiple NICS or multiple IP addresses.

Multilink Protocol (MP) — Used to combine multiple physical links into a single logical link. For example, you could use MP to combine two 56-KB modem links into a 128-KB link.

name query response — Response sent from a WINS server to the WINS client, either informing the client of the NetBIOS name to IP address resolution or of failure to achieve a resolution.

name registration company — Company with the authority to register DNS domains within the DNS namespace.

NAT editor — Installable component that modifies packets so NAT can translate them. Windows 2000 includes built-in NAT editors for protocols, including FTP, ICMP, PPTP, and NetBT.

NAT interface — Virtual interface in the RRAS snap-in that represents an actual private or public network interface on the NAT server.

native mode — Mode used by Windows 2000 domain controllers when the entire network consists of only Windows 2000 servers and Active Directory-aware clients.

nbtstat — Command-line tool that displays NetBIOS over TCP/IP information.

Net Shell (netsh) — Command-line tool used to configure and monitor Windows 2000 networking components, including RRAS.

NetBIOS — Session-level API developed to provide high-level applications with easy access to lower-level networking protocols.

NetBIOS Enhanced User Interface (NetBEUI) — Small, fast, efficient, nonroutable protocol stack used in small networks only.

NetBIOS name query — Used by WINS clients to query WINS servers for information about a particular NetBIOS name; in short, used to find NetBIOS name to IP address mappings.

NetBIOS name registration — Sent by WINS clients to WINS servers to ask for registration of a particular NetBIOS name with an IP address.

NetBIOS name release — Sent by WINS clients to direct the WINS server to terminate the dynamic mapping of a NetBIOS name to an IP address.

NetBIOS name renewal — Sent by WINS clients to request that the WINs server extend NetBIOS name to IP address mapping; normally occurs halfway through the TTL.

NetBIOS Name Server (NBNS) — Server configured with the WINS server service.

NetBIOS over TCP/IP — NetBIOS using TCP/IP as its lower-level networking protocol stack.

NetBIOS scope — Optional parameter used to break NetBIOS domains into smaller sections; similar to subnets in TCP/IP

NetBT — Common abbreviation for NetBIOS over TCP/IP

netdiag — New command-line tool in Windows 2000 that tests a large portion of the networking components on a machine. Provides much of the same information as other command-line tools such as netstat, nbtstat, and ipconfig.

netstat — Command-line tool that provides information about current TCP/IP connections.

Netware Core Protocol (NCP) — Primary upper-layer protocol in IPX/SPX that facilitates client/server interaction.

Netware Link State Protocol (NLSP) — More advanced link state routing protocol in the IPX/SPX protocol stack Designed to replace the RIP protocol.

Network Address Translation (NAT) — Network service used to "translate" between public TCP/IP addresses and private internal addresses specified in Request for Comments 1918.

network driver interface specification (NDIS) — Boundary layer in the Windows 2000 networking architecture that serves as an intermediary between the networking protocols and the Data Link layer drivers and network interface cards.

Network ID — Portion of an IP address that represents the bits reserved for the network number.

Network Monitor — Tool that comes with Windows 2000 and allows you to capture and view data packets passing over the network.

network operating system (NOS) — Computer software designed to provide network services to clients.

networking protocols — Standard language used by two computers to communicate over a network. Networking protocols define how information is fragmented and shaped for passage over the network.

non-broadcast multiple access (NBMA) router — Router that can communicate with other routers without broadcasting.

objects — Components found within the Active Directory structure; an object represents each network resource in the Active Directory structure

Open Shortest Path First (OSPF) — Link-state routing protocol that enables routers to exchange routing information. Called a link-state protocol because it actually creates a map (a routing table) of the network that calculates the best possible path to each network segment by maintaining information on the state of links (whether they are up or down).

Open System Interconnection model (OSI model) — Seven-layer conceptual model designed to help standardize and simplify learning, implementing, and creating network communication between two network hosts.

Options — Extra IP configuration parameters that can be given to DHCP clients when they lease an IP address.

p-node — NetBIOS node type that uses directed communication to a WINS server to resolve NetBIOS names to IP addresses.

Packet Internet Groper (ping) — Command-line tool used to test connectivity between two IP hosts.

Password Authentication Protocol (PAP) — Authentication method that transmits a user's name and password over a network and compares them to a table of name-password pairs.

pathping — Command-line tool that combines ping and tracert functions with new statistics reporting functions.

plug and play support — Ability of an operating system to automatically detect and install drivers for devices that conform to plug and play standards; simplifies hardware device management and installation.

Point-to-Point Protocol (PPP) — Remote-access protocol used to establish a connection between two remote computers. RRAS supports PPP for dialing both in and out.

pointer (PTR) resource records — Map an IP address to a fully qualified domain name (FQDN). *See also* reverse lookup records.

pre-shared keys — Passwords entered into each computer communicating with IPSec. As long as both computers are configured with the same pre-shared key, they trust one another.

pre-shared key — Single key used both to encrypt and decrypt data. This key is often a simple password shared beforehand by both the encrypting and decrypting parties.

primary name servers — DNS servers that hold a read/write copy of the zone file for a particular DNS zone; control replication with secondary name servers.

private address — Any address belonging to one of the three ranges of IP addresses designated as private by Internet authorities. A host with a private address may only communicate with hosts on the Internet through a service such as NAT.

private key — Part of a public/private key pair kept secret, the private key is only available to the person who holds the key.

protocol stack — Group of protocols working together to complete the network communication process.

Public address — Any address not belonging to one of the three ranges of IP addresses designated as private by Internet authorities.

public key — Part of a public/private key pair made publicly available.

public key certificates — Provided by a certificate authority. Each end of the IPSec connection uses the other end's public certificate for authentication.

public key encryption — Encryption method in which a recipient's public key encrypts data and then that same recipient's key decrypts the data.

public key infrastructure (PKI) — System of components working together to verify the identity of users who transfer data on a system and to encrypt that data if needed.

pull replication — Replication of the WINS database that occurs at a preset time interval; used with slow WAN links.

push replication — Replication of the WINS database that occurs after a predetermined number of changes to the database occur; used with fast connections between replication partners.

Recovery Agent — User designated as able to access the EFS Recovery Keys on a computer. By default, this is the administrator.

recursive query — DNS query which asks the server to respond either with the DNS information or an error message stating that it does not have the information; used between clients and DNS servers.

remote access — Broadly defines the ability of one computer to connect to another computer over a dial-up or other WAN connection and to access resources remotely.

remote access profile — Associated with policies and containing settings that determine what happens during call set up and completion.

remote access policy — Used to configure conditions under which users may connect using a specific remote access connection. You can include restrictions based on criteria such as time of day, type of connection, authentication, and even length of connection.

remote access protocols — Define the way in which one computer connects to another computer over a WAN link. PPP and SLIP are the two main remote access protocols in use today, though the newer and stronger PPP is much more common.

Remote Authentication Dial-In User Support (RADIUS) — Authentication and accounting system used by many ISPs to verify user credentials and log user activity while the user is connected to a remote system.

remote control — Process in which a client computer connects to a remote server and actually takes control over that server in a separate window on the client computer. Activities within this window seem to occur as if the user is actually sitting at the server computer. All applications run on the server. RRAS does not support remote control, only remote access.

Request for Comments (RFC) — Proposals presented to the Internet community describing everything from possible TCP/IP standards to simple informative tracts.

reservations — Using the MAC address of the client to ensure that a particular IP address is always leased to that client.

Reserved client options — Scope options created for a single client that has been given a DHCP reservation.

reverse lookup records — Another name for PTR records. These records resolve a host name from a known IP address.

reverse lookup zones — Special DNS zones that holds PTR records, IP address to host name mapping.

RIPv1 — Simple-to-use and well-supported interior routing protocol. RIP is a distance vector routing program, meaning that it not only supplies information about the networks a router can reach, but supplies information about the distances to those networks as well.

RIPv2 — Protocol developed to address several shortcomings in RIPv1, for example, by providing a multicast option in addition to broadcasts for routing announcements and by including the subnet mask in announcements.

Rivest-Shamir-Adleman (RSA) algorithm — Most common public key encryption algorithm in use today, and the MCS default.

root CA — CA at the top of a CA hierarchy and trusted unconditionally by a client.

root name servers — Servers that hold information about the overall Internet domain name servers.

ROUTE command — Command-line utility used to manipulate static entries in a routing table.

router — Device used to connect different IP subnets and to route data between them.

Routing Information Protocol (RIP) — Routing protocol provided with the IPX/SPX protocol stack.

Routing and Remote Access Service (RRAS) — Windows 2000 service that provides remote access and routing functionality to remote clients.

routing table — List of networks that the system knows about and the IP addresses of routers that packets must pass through to get to those networks.

Scopes — Ranges of IP addresses configured for lease to clients via DHCP.

scope options — Options that apply to all clients in one scope only.

secondary name servers — DNS servers that hold read-only copies of a zone file for a particular DNS zone; accept updates to the DNS zone file only from configured primary name servers.

security association — Defines the common security mechanisms, such as keys, that two computers use to create the IPSec connection.

Sequenced Packet eXchange (SPX) — Layer four protocol that provides guaranteed delivery; similar in function to TCP.

Serial Line Interface Protocol (SLIP) — Older protocol developed in UNIX and still in wide use today. Windows 2000 RRAS supports SLIP in dial-out configurations, but you cannot use a SLIP client to dial in to an RRAS server.

serial links — Generally slow-speed connections used for wide area network connectivity.

server options — Options that apply to all clients in all scopes configured on a DHCP server.

Service Advertisement Protocol (SAP) — Protocol used on IPX/SPX networks by clients to find network services and by servers to advertise network services.

Shiva Password Authentication Protocol (SPAP) — Included mainly for compatibility with remote access hardware devices manufactured by Shiva, a private company now owned by Intel. SPAP isn't really used much on most networks.

Simple Mail Transfer Protocol (SMTP) — Application layer TCP/IP protocol that provides mail delivery services.

SOHO — Acronym that stands for Small Office/Home Office. SOHO networks are considered the main beneficiaries of ICS and NAT. Though they vary a great deal in configuration, a SOHO network, as defined by Microsoft, has one network segment, uses peer-to-peer networking, and supports TCP/IP.

Stand-alone CA — Used to issue certificates to users outside the enterprise and does not require access to the Active Directory.

static assignment — Manually assigning an IP address to a host.

static mappings — Define in advance how to map certain addresses and ports instead of letting mapping happen automatically. Although you can create static mappings for outbound traffic, the most common reason to use a static mapping is to host some form of Internet service (that is, Web server, FTP server, and so on) on a private computer.

static router — Router to which routes must be added manually using either the ROUTE command or the RRAS snap-in.

subnet mask — 32-bit number used to determine the portion of an IP address that represents the network ID and the host ID.

subnetting — The process of borrowing host bits to increase the number of network bits.

subordinate CA — CA beneath the root CA in the CA hierarchy and perhaps even under other subordinate CAs. Subordinate CAs typically issue certificates to users and computers in the organization

superscopes — Multiple scopes grouped together to allow centralized management; also allow for more than one range of IP addresses on a single physical subnet.

telnet — Application layer protocol in TCP/IP that allows a user to log on to a remote host and execute programs remotely.

terminal services — Services that allow a server to host applications for clients; with terminal services, clients no longer used to run applications can act as dumb terminals for applications on a terminal server.

Tombstoned — State of a WINS entry once it is marked for deletion.

tracert — Trace route command-line tool that allows testing of the entire path between two hosts.

transit internetwork — Basic IP infrastructure over which a Virtual Private Network is created. Typically, the transit internetwork is the Internet itself, though other IP networks may be the transit internetwork.

Transmission Control Protocol (TCP) — Transport layer protocol in the TCP/IP protocol stack that is connection-oriented and reliable; provides guaranteed delivery.

Transmission Control Protocol/Internet Protocol (TCP/IP) — Suite of networking protocols designed to transfer data between computers on the Internet. TCP/IP is becoming the most popular networking protocol used on private networks, as well.

transport device interface (TDI) — Boundary layer in the Windows 2000 networking architecture between networking protocols and the upper-layer services.

transport mode — Mode in which the two endpoints of IPSec communication are two computers that have IPSec configured. For this mode to work, both computers must use the TCP/IP protocol.

Trivial File Transfer Protocol (TFTP) — Like FTP, provides file transfer between two TCP/IP hosts; TFTP uses UDP as its transport protocol and is faster, but more unreliable than FTP.

tunnel mode — Mode in which two communicating computers do not use IPSec themselves. Instead, the gateways connecting each client's LAN to the transit network create a virtual tunnel that uses the IPSec protocol to secure all communication that passes through it.

unique NetBIOS names — NetBIOS names assigned to a single computer and its associated services.

Universal Serial Bus (USB) — Hardware specification that allows for hot insertion and removal of hardware devices.

User Datagram Protocol (UDP) — Connectionless, best-effort delivery transport layer protocol in the TCP/IP stack.

user-defined option classes — Allow expansion of DHCP options to include parameters determined by the network administrator for a particular client.

user profile — Information associated with a user account. Profiles of users who are members of a Windows 2000 domain are stored in the Active Directory, and profiles of users who are not members of a domain are stored on the local computer.

vendor-defined option classes — Expanded DHCP options created for one particular vendor's computers or network hardware.

Virtual Private Networking (VPN) — Secure, logical network constructed directly between a VPN client and a VPN server on top of a physical transit internetwork such as the Internet.

wide area network (WAN) — Network or collection of networks spread across a large geographical area.

Windows 2000 Advanced Server — Enterprise or large department version of Windows 2000; supports clustering and eight-way multiprocessor systems with up to 8 GB of RAM.

Windows 2000 DataCenter Server — Data warehouse or extremely large-scale version of Windows 2000; designed for processor intensive simulations or massive processing tasks; supports up to 32 processors with 64 GB of RAM in special original equipment manufacturer versions.

Windows 2000 Professional — Client version of the Windows 2000 product family; designed to provide a stable, reliable, and fast platform for end users to run their applications.

Windows 2000 Server — Small department or workgroup version of Windows 2000; supports four-way multiprocessor systems with up to 4 GB of RAM.

Windows Internet Name Service (WINS) — Windows 2000 service that provides a dynamic database of NetBIOS name to IP address mapping.

Windows Internet Naming Service (WINS) — Network service that provides NetBIOS name to TCP/IP address resolution.

WINS replication — Process of replicating the WINS databases between two WINS servers.

X.509 certificate — Most widely used format for certificates, as defined by the International Telecommunications Union (ITU) in Recommendation X.509.

zone of authority — Portion of the DNS namespace that an organization controls.

zones transfers — Copying zone file information from primary name servers to secondary name servers.